UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/357,483	07/20/1999	STEPHEN MICHAEL MATYAS JR.	5577-170	9314

20792 7590 11/20/2003

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 11/20/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/357,483	MATYAS ET AL.	
	Examiner	Art Unit	
	Paula W Klimach	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 August 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *6* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 8/27/2003 (Paper No. 7). Original application contained Claims 1-27. Applicant added Claims 28-57, and amended Claims 1,10, 17, 22, 24, and 27. Applicant made the necessary changes to the specification for the withdrawal of the objection to the specification. The amendment filed on 8/27/2003 have been entered and made of record. Therefore, presently pending claims are 1-57.

Response to Arguments

Applicant's arguments filed 8/27/2003 have been fully considered but they are not persuasive because of following reasons.

Applicant argued, "... *the prior art reference or references when combined must teach or suggest all the recitation of the claims.*" This is not found persuasive. The obtaining of the first and second secret seed values; obtaining the third publicly known randomization value; and dividing a potential range of RSA encryption values into a first interval and a second interval are used to determine select the RSA cryptographic value p such that p is in the first interval of the RSA encryption values. The same function is carried out such that q is in the second portion of the interval. Rivest discloses that to gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits (page 9 section B paragraph 4). By finding p and q in different intervals p and q would have different values and therefore different lengths. The size of the range in the interval would determine the difference in length.

Applicant argued further, "*...there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art,*

to modify the reference or to combine reference teachings." This is not found persuasive. In the office action filed 5/23/03 the motivation for combining Rivest and Borza in reference to claim 1 is, "because it would reduce the chances of predicting the random number (column 3 lines 25-29 Borza)." Rivest discloses that p and q are large "random" primes used for RSA key generation. However Rivest does not discuss the method used to find the random numbers. Borza discloses how to find the random number using user specific information in the form of a biometric. As a result the two references are combined to show that the random number used in Rivest can be found using the method disclosed by Borza.

Claim Rejections - 35 USC § 101

The 101 rejection against claims 1-20 are withdrawn because the office interprets the claims to be "A computer implemented method of generating the RSA cryptographic values..."

Claim Rejections - 35 USC § 103

1. **Claims 1-7, 11-33, 37-48, and 52-57** are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of Borza et al (6,215,874 B1).

In reference to claims 1, 22, and 25, Rivest discloses a system for finding RSA values, abstract. On page 9, Rivest discloses that p and q are large "random" primes used for RSA key generation. However Rivest does not discuss the method used to find the random numbers. Obtaining the first and second secret seed values; obtaining the third publicly known randomization value; and dividing a potential range of RSA encryption values into a first interval and a second interval are used to determine select the RSA cryptographic value p such that p is in the first interval of the RSA encryption values. The same function is carried out such that q is in the second portion of the interval. Rivest discloses that to gain additional protection against

sophisticated factoring algorithms, p and q should differ in length by a few digits (page 9 section B paragraph 4). By finding p and q in different intervals p and q would have different values and therefore different lengths. The size of the range in the interval would determine the difference in length.

Borza discloses a method and system for generating random numbers, abstract, that uses biometrics, column 4 lines 28-31.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the biometric random number generator to find the two large random primes for RSA. One of ordinary skill in the art would have been motivated to do this because it would reduce the chances of predicting the random number, column 3 lines 25-29.

In reference to claims 2, 28, and 43, Rivest discloses a method of finding the prime divisors p and q, page 9.

In reference to claim 3, 11, 12, 29, and 44, the prime divisors are generated using random numbers. Borza discloses the random number generation as being based on a biometric. The Borza random number generator based on a fingerprint whose image is taken by a biometric sensing device, column 4 lines 29-51.

In reference to claim 4, 30, and 45, wherein the steps of generating auxiliary prime divisors comprises the steps of concatenating the first secret seed value (W_p), the second secret seed value (W_q) and the third randomization value (IV) so as to provide an exponent value (X); determining an initial random value by determining $Y = g^X(\mathrm{mod}p_o)$; setting the most significant bit of the initial prime search values to "1" to provide final prime search values; and selecting as the prime divisors the smallest prime value greater than or equal to the final prime search values.

The randomness of the value IV and therefore X determines the security of the encryption algorithm. In standard RSA the values that are prime numbers also increase the security of the algorithm. Thus the added mathematical computation using the random number X may determine the size of the random number, which is a design decision.

In reference to claim 5, 31, and 46, wherein at least one of a new first secret seed value (W_p), a new second secret seed value (W_q) and a new third randomization value (IV) if the length of at least one of the prime divisors is greater than the length of the final prime search values; and re-generating the prime divisors if the length of at least one of the prime divisors is greater than the length of the prime search values. Rivest discloses that to gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits (page 9 section B paragraph 4). By finding p and q in different intervals p and q would have different values and therefore different lengths. The size of the range in the interval would determine the difference in length.

In reference to claim 6, 7, 32, 33, 41, 47, 48, 56, wherein the initial prime search values have a first length if a public encryption exponent (e) has an odd value and a second length of the public encryption exponent (e) has an even value. The length of the prime search value is easily controlled in the design of the encryption system.

In reference to claims 13, 14, 37, 38, 52, and 53, wherein determining if a candidate for p and q are considered outside the range of RSA cryptographic values of the entity specific segment, and selecting new secret seed values, and a new third randomization values. This would determine a new range or interval for the values of p and q. Rivest discloses that to gain additional protection against sophisticated factoring algorithms, p and q should differ in length

by a few digits (page 9 section B paragraph 4). By finding p and q in different intervals p and q would have different values and therefore different lengths. The size of the range in the interval would determine the difference in length.

In reference to claims 15, 39, 42, 54, and 57 wherein the steps of generating a first intial value comprise the steps of mixing using a publicly known function to determine the first intitial value and the second initial value. Rivest discloses that to gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits (page 9 section B paragraph 4). By finding p and q in different intervals p and q would have different values and therefore different lengths. The size of the range in the interval would determine the difference in length.

In reference to claims 16, 23, and 26, it is well known that an authentication process includes generating keys that are compared to the expected keys. The keys are determined by the randomized values p and q and therefore the authentic owner would have p and q or a function of p and q.

In reference to claims 17, 24, and 27, Rivest discloses a method of recovering the cryptographic values p and q by factoring n since it can be done easily once d is known (page 12 section C paragraph 2). The comparison is then an elementary mathematic computation. It is well known that an authentication process includes generating keys that are compared to the expected keys. The keys are determined by the randomized values p and q and therefore the authentic owner would have p and q or a function of p and q.

In reference to claims 18, 40 and 55, it is well known that an authentication process includes generating keys that are compared to the expected keys. The keys are determined by

the randomized values p and q and therefore the authentic owner would have p and q or a function of p and q.

In reference to claims 19, 20, and 21, wherein the first of the two prime numbers is a smaller of the two prime numbers. Rivest discloses that to gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits (page 9 section B paragraph 4). By finding p and q in different intervals p and q would have different values and therefore different lengths. The size of the range in the interval would determine the difference in length.

2. **Claims 8-10, 34-36, and 49-51** is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest and Borza as applied to claim 1 above, and further in view of Soutar et al (6,219,794).

Rivest discloses a method of generating RSA cryptographic values, and Borza discloses a method of generating a random number using a biometric. However, neither Borza nor Rivest discloses a method for using a biometric by calculating a value using the biometric information to create a biometric template.

Soutar discloses a method for using a biometric by calculating a value using the biometric information to create a biometric template, Fig. 1.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Soutar method to calculate a biometric template. One of ordinary skill in the art would have been motivated to do this because the key cannot be released from the protected filter other than via the interaction with the correct biometric image, Soutar abstract.

In reference to claim 9, 35, and 50, wherein the RSA cryptographic values comprise n bits and wherein the first interval comprises RSA cryptographic values. The length of the intervals determines the size of the prime numbers. Rivest discloses that to gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits (page 9 section B paragraph 4). By finding p and q in different intervals p and q would have different values and therefore different lengths.

In reference to claims 10, 36, and 51, wherein the binary size of the RSA cryptographic values are 2n, a size m is n-b-2 and wherein the step of mapping the first initial value comprises the steps of linearly mapping the values onto the entity specific information to arrive at two intervals. The intervals determine the size of the prime numbers. Rivest discloses that to gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits (page 9 section B paragraph 4). By finding p and q in different intervals p and q would have different values and therefore different lengths. The function is a design decision for creating a template from a biometric.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Rivest	A method for Obtaining Digital Signatures and Public-Key Cryptosystems
Borza et al	6,215,874 B1
Soutar et al	6,219,794

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Fri 7:15 a.m to 3:45 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100